Organizzazione

- Compitini di valutazione
- Progetti:
  - Appunti dalle lezioni
  - Presentazione di argomenti specifici
  - Laboratorio
- Interazione
- Commenti benvenuti

Disponibilità materiale

http://www.dia.unisa.it/~ads/corso-security/www

Crittografia

- Introduzione
- Crittografia Classica (+ Enigma)
- Crittoanalisi (+ Vigenere programma)
- DES, modalità, Triplo DES
- Altri cifrari a blocchi (IDEA, RC5,…)
- AES (+ MARS)
- Stream Cipher (+ A5)
- Crittografia a chiave pubblica
- Distribuzione di chiavi
- Key Escrow
- Firme Digitali
- Tecniche per autenticazione ed integrità (Funzioni Hash, MAC)
- Identificazione (password)
- Identificazione (schemi)
- Identificazione biometrica
- Generazione pseudo-casuale
- Condivisione di segreti
- Crittografia Visuale
- Protocolli

Sicurezza Dati

- Sicurezza nei Sistemi Operativi (Unix)
- Sicurezza nei Sistemi Operativi (Windows NT)
- TCP/IP
- HTTP e S-HTTP
- PKI
- E-mail (PEM, PGP)
- SSL
- Anonimia
- Firewall
- IPsec
- Java
- Script ostili
- Codice *malizioso* (Virus, Worm)
- Commercio Elettronico (Moneta elettronica, iKP)
- SET
- Watermark
- Sicurezza Data Base
- Smart Card
- GSM, WAP
- Amministrazione Sicurezza (Analisi rischi, Politiche,…)
- Standard, norme ed RFC

Sicurezza su Reti

- Sniffer
- Denial of Service
- Monitoring attivo utenti
- Network scanner